REMARKS

Claims 29-48 were presented for examination and were pending in this application. In an Office Action dated December 1, 2004, claims 29-48 were rejected. Applicants thank Examiner for examination of the claims pending in this application and addresses Examiner's comments below. Applicants also thank Examiner and his Primary Examiner for the interviews on February 23, 2005 and March 17, 2005. The substance of those interviews is incorporated by reference per the Interview Summary mailed on February 25, 2005, and MPEP § 713.04.

Applicants herein amend claims 29, 36, and 43. No claims are canceled or added. The claim changes are believed not to introduce new matter, and their entry is respectfully requested. The claims have been amended to expedite the prosecution of the application in a manner consistent with the Patent Office Business Goals, 65 Fed. Reg. 54603 (Sept. 8, 2000). In making these amendments, Applicants have not and do not narrow the scope of the protection to which Applicants consider the claimed invention to be entitled and do not concede that the subject matter of such claims was in fact disclosed or taught by the cited prior art. Rather, Applicants reserve the right to pursue such protection at a later point in time and merely seeks to pursue protection for the subject matter presented in this submission.

Based on the above Amendment and the following Remarks, Applicants respectfully request that Examiner reconsider all outstanding objections and rejections, and withdraw them.

Response to Rejection Under 35 USC 103(a) in View of Alsberg and Oliver

In the 4th paragraph on page 2 of the Office Action, Examiner rejects claims 29-30, 33, 36, 38, 41-44, and 47 under 35 USC § 103(a) as allegedly being unpatentable in view of U.S. Patent No. 4,672,572 to Alsberg ("Alsberg") and U.S. Patent Application No. 2002/0133412 to Oliver et al. ("Oliver"). Applicants respond as set forth below.

Per the Examiner interview, representative claim 29 has been amended to now recite,

> A method for use in a detector device for controlling access to information on a network including a plurality of interconnected devices, the detector device coupled to the network between a first device and a second device, the method comprising:
>
> monitoring, independent of the first device and the second device, a plurality of request signals for data between the first device and the second device in the network, at least one request signal including a user identification parameter;
>
> determining whether a user identified by the user identification parameter in the at least one request signal is permitted access to the data being requested;
>
> comparing a predetermined parameter associated with the user with a predetermined parameter associated with the data to determine permission to access the data; and
>
> generating a response to the request signal to alter communications between the first device and the second device in response to the comparison providing a first result and not altering communications between the first device and the second device in response to the comparison providing a second result, the detector device allowing the plurality of request signals to pass uninterrupted between the first device and the second device regardless of the first result or the second result in response to an operational failure of the detector device, the operational failure comprising a non-functioning operation.
>
> (emphasis added).

The claimed invention beneficially recites a method that allows for monitoring communications between two devices, independent of those devices. The method also determines whether a user identified by a user identification parameter in a request signal is permitted access to requested data. In particular, the method includes comparing a

predetermined parameter associated with the user with a predetermined parameter associated with the data to determine permission to access the data.

If the comparison produces a first result, the method generates a response to the request signal to alter communications between the first device and the second device. If the comparison generates a second result, no communications are altered between the first device and the second device. Moreover, the claimed invention beneficially allows for the two devices to communicate with each other regardless of the first result or the second result in response to an operational failure of the detector device. This operational failure includes a non-functioning operation of the detector device. Hence, the claimed invention provides a robust monitoring and processing system without introducing a point of failure within a network.

The claimed invention finds support in the specification at, for example, page 4, line 8 to page 6, line 10, page 8, line 13 to page 9, line 7, page 10, lines 16-27, page 11, lines 6-19, and Figures 2 and 3. These portions of the specification describe how a detection device (or "injector") monitors communication between a client and a server and based upon a user (e.g., a client machine) request to seek access to information on a server (e.g., restricted site), the detection device alters communication between the two devices by sending a reset signal to the server, which prevents further replies from being sent back to the client machine. Moreover, the claimed invention also finds support for its operation in the context of an operational failure in, for example, Figure 2 and page 10, line 28 to page 11, line 5, which notes passage of traffic regardless of functional status of the detection device. In addition, Figures 4 and 5, and their corresponding description, provide additional support for the claimed invention in the context of exemplary operational environments.

The combination of Alsberg and Oliver fail to disclose, suggest or teach the claimed invention. Alsberg discloses "a protector device [] for enhancing the security of a computer system which includes one or more user terminals in one or more host computers." (Alsberg, Abstract). Alsberg goes on to disclose that the "projector device includes a detection means for monitoring communications between the terminals and the host computers in which the detection means is independent from the host computers in the terminal but is connected to the computers and terminals such that certain information transmitted between the computers and the terminals is transmitted through the detection means." (Id.).

As discussed in the Examiner interview, the access node 12, 14 (considered the detection means) in Alsberg is an inline device. As an inline device, packets must go through the access node 12, 14 in order to communicate with the appropriate servers. Specifically, Alsberg notes that the access node "typically consists of a serial in/out controller 26. The controller 26 receives and transmits asynchronous signals from a plurality of user terminals 16 of FIG. 1 and causes the actual physical connects and disconnects to occur between the terminals and the access node." (Emphasis added). (Alsberg, col. 4, lines 44-50; Fig. 2). Thus, the access node 12, 14 in Alsberg necessarily introduces a point of failure in the disclosed network. In contrast, the claimed invention monitors the communication between a first device and a second device, and in response to that monitoring activity can take certain action as is claimed (as well as described in the specification, for example, with respect to Figure 3).

In addition, Alsberg also notes that the access node includes a central processing unit (CPU) 30 that in order to "comprehend some of the functions [of] the access node CPU 30 it may be desirable to refer to FIG. 3 which is a functional diagram of the access-node

software." (Alsberg, col. 4, lines 62-63; col. 5, lines 9-13). Figure 3 shows a "command protocol interpreter (CPI) 40 [that] serves several functions. First and foremost, the CPI is responsible for maintaining and controlling connections between its serial lines and the serial lines on other access nodes, possibly on other networks, as well as to a security server." (Id., col. 5, lines 18-23; Fig. 3). Thus, the access node disclosed in Alsberg is essential for communication within the context of its disclosed system because permission must first be granted to establish communication and thereafter physical connection would be established; if there is no permission, or it is refused, the communication is dropped, and hence the physical connection is dropped. This further highlights how the access point in Alsberg introduces a point of failure unlike the claimed invention.

Referring next to Oliver, it fails to address the deficiencies of Alsberg, for example, allowing request signals to pass between devices even in the event of an operational failure of the detector device. As has been discussed in prior responses, Oliver discloses a system in which monitoring software is located on a customer backend to collect data. Such approaches are conventional data monitoring approaches that require dependence between the monitor and an end node, for example, the monitor and a server, both at a technology and business relationship level. In Oliver, the "CALS system [detection system] is not located between a first device, i.e., the CMa end-user system, and a second device, i.e., the CSPa server system. (Oliver, ¶ 149, 306-310, 344, 347, 373 (location of structures and operation of system)). Rather, the CALS system is located behind the server CSPa, *i.e.*, the back-end of the system. The reason the CALS system is on the back-end is because it controls access to the CSPa server in terms of whether or not to grant access to the end user-system Cma so

Cma can establish a connection with the server CSPa. Hence, the CALS system in Oliver is not between a first device and a second device.

Next, citation in Oliver to paragraphs 0341 to 0347 discloses no more than conventional back end password authentication type processes. Oliver adds no more than a conventional authentication process to the security system that determines whether or not to allow physical connections as disclosed in Alsberg. More importantly, assuming arguendo that the two references can be combined, Oliver still fails to address the fundamental shortcomings of Alsberg, which includes introduction of a point of failure within the network. Rather, Oliver itself retains the same problem because if the authentication process in Oliver breaks down, communication between devices cease.

Thus, for at least the reasons set forth above, representative claim 29 is patentably distinguishable over the cited references. Applicants respectfully request reconsideration of the basis for the rejection and request allowance of the claims (claims 29, 36, 43 and their respective dependencies) at this time.

Response to Rejection Under 35 USC 103(a) in View of Alsberg, Oliver and Iwamura and Alsberg, Oliver, and Lyles

In the 22nd paragraph on page 6 of the Office Action, Examiner rejects claims 31-32, 35, 37, 39-40, and 45-46 under 35 USC § 103(a) as allegedly being unpatentable in view of Alsberg, Oliver, and U.S. Patent No. 6,272,535 to Iwamura ("Iwamura"). Claims 34 and 48 are rejected under 35 USC § 103(a) as allegedly being unpatentable in view of Alsberg, Oliver, and U.S. Patent No. 5,917,822 to Lyles et al. ("Lyles").

Applicants note the arguments set forth above with respect to Alsberg and Oliver apply to these claims and are herein incorporated by reference. As for Iwamura, its

disclosure fails to address the deficiencies of Alsberg and Oliver. Moreover, like Alsberg and Oliver, Iwamura is not independent of the devices it monitors. Specifically, Iwamura notes, "the accounting apparatus has a money input, by which a user can input an amount of money into the apparatus." (Iwamura, Abstract). That is, the system and process in Iwamura must have both a technological and business relationship with the user and cannot be independent in a manner as recited in Applicants' claimed invention.

Likewise, Lyles also fails to address the deficiencies of Alsberg and Oliver. Lyles discloses a system and method "executed by or in a head-end controller." (Lyles, Abstract). As with Oliver and Iwamura, Lyles too requires a technological and business relationship with an end node, here a head-end service provider, and cannot be independent in a manner as recited in Applicants' claimed invention. Further, although Iwamura and Lyles may disclose particular components in isolation, they fail to address the deficiencies of the primary references (e.g., allow communication between devices when an operational failure occurs within a detector device), let alone whether there is any appropriate teaching or suggestion to combine the references in a manner as is claimed by Applicants.

Thus, based on the above Amendments and Remarks, Applicants respectfully submit that for at least these reasons claims 31-32, 35, 37, 39-40, and 45-46 are also patentably distinguishable over the cited references, both alone and in combination. Therefore, Applicants respectfully request that Examiner reconsider the rejections, and withdraw them.

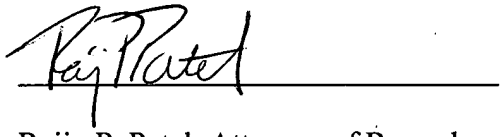
Conclusion

Applicants also note (as briefly discussed with Examiner on March 30, 2005), that they are enclosing with this Amendment and Response an information disclosure statement as is required per 37 CFR § 1.56. Applicants respectfully note that the claims as presented

herein are believed to be patentably distinguishable over the cited references as submitted with this information disclosure statement and as have been cited throughout the prosecution of this application. Reconsideration of the rejections and allowance of the pending claims is respectfully requested.

Applicants respectfully invite Examiner to contact Applicants' representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,
Stanislav Khirman, Mark Ronald Stone, Oren Arial and Ori Cohen

Date: March 31, 2005 By: 

Rajiv P. Patel, Attorney of Record
Registration No. 39,327
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7607
Fax: (650) 938-5200